(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－102240

(43)公開日　平成11年(1999)４月13日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	1/26		Ｇ０６Ｆ	1/00	３３４Ｂ
	1/00	３７０			３７０Ｅ
	3/02	３４０		3/02	３４０Ａ
	15/00	３３０		15/00	３３０Ｂ

審査請求　有　　請求項の数15　ＯＬ　（全 10 頁）

(21)出願番号　特願平10－141510

(22)出願日　平成10年(1998)５月22日

(31)優先権主張番号　８６１０７３６１

(32)優先日　1997年５月30日

(33)優先権主張国　台湾（ＴＷ）

(71)出願人　595039162
華邦電子股▲ふん▼有限公司
台湾新竹科學園區研新三路４號

(72)発明者　王　政　治
台湾新竹縣竹北市新庄里110－９號

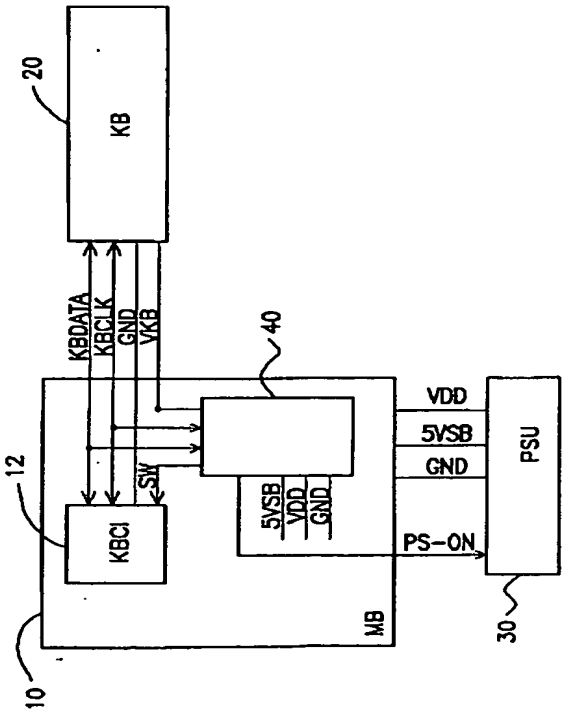
(74)代理人　弁理士　曾我　道照　（外６名）

(54)【発明の名称】　コンピュータ用電源のセキュリティ制御装置

(57)【要約】

【課題】　パスワード入力の妥当性に基づいてコンピュータ・システムへの主電力供給を開始するか否かを決定するコンピュータ用電源のセキュリティ制御装置を得る。

【解決手段】　コンピュータ・システムへの無許可アクセスに対するシールディングを提供するために、コンピュータ・システムのパワーオン・セキュリティ制御装置が開示されている。従来装置のオペレーティング・システム・レベルではなく、ファームウェア・レベルの保護が提供される。コンピュータ・システムのパスワードの試行入力プロセスでは避けられないパワーオン／オフ・サイクルの繰り返しを全体として回避し、パスワードの反復試行が試みられる間にコンピュータ中の精密なサブシステムに損傷が与えられ得るという危険性を低減させる。



1

【特許請求の範囲】

【請求項１】　メインボード回路系、電源、およびキーボードを有するコンピュータ・システム用のパワーアップ・セキュリティ制御を行うコンピュータ用電源のセキュリティ制御装置であって、

前記コンピュータ・システムがオフである時に、前記メインボード回路系のキーボード制御装置インタフェースと前記キーボードとの間で通信するキーボード信号を代行受信するキーボード代行受信ユニットと、

前記キーボード代行受信ユニットが代行受信したキーボード信号を、受信してデコードするキーボード入力データ・デコーダと、

前記キーボード入力データ・デコーダの出力側に供給されたキーボード信号のデコード済みデータを、所定フォーマットで記憶する先入れ先出しバッファと、前記コンピュータ・システムのパワーアップ許可を指定するようにプリセットされたパスワードを記憶するパスワード・メモリと、

前記先入れ先出しバッファおよび前記パスワード・メモリのそれぞれの出力端子に接続された２つの入力端子を有し、前記キーボード信号および前記プリセット・パスワードの突合せを比較し、前記比較の突合せ条件を示す信号を生成する比較ユニットと、

前記比較ユニットが生成した突合せ条件を受信して、前記突合せ条件の論理状態に基づいて制御信号を生成し、前記突合せ条件の結果が正であれば前記コンピュータ・システムの電源をパワーアップするように制御する電源制御ユニットとを備えたコンピュータ用電源のセキュリティ制御装置。

【請求項２】　前記電源制御ユニットは、前記比較ユニットが比較の結果として正の突合せ条件を生成した時に、前記コンピュータ・システムに電力を供給する電源を開始し、前記比較ユニットが比較の結果として負の突合せ条件を生成した時に、前記電源をパワーオフ状態で維持する請求項１に記載のコンピュータ用電源のセキュリティ制御装置。

【請求項３】　前記コンピュータ・システムの電源は、イネーブル入力端子を含み、前記電源制御ユニットが電源を開始して前記コンピュータ・システムをパワーアップするために前記電源のイネーブル入力端子にイネーブル信号を出力した時に、前記電源が開始される請求項１に記載のコンピュータ用電源のセキュリティ制御装置。

【請求項４】　前記電源制御ユニットは、論理回路系をさらに含み、前記突合せ条件の結果および前記コンピュータ・システムの主スイッチの論理状態に基づいて実行された論理演算の結果を出力する請求項２に記載のコンピュータ用電源のセキュリティ制御装置。

【請求項５】　前記電源は、ＡＴＸ標準に従うものであり、

前記電源制御ユニットは、前記突合せ条件および前記コンピュータ・システムの主スイッチの論理状態に基づいてＮＡＮＤ演算を実行する論理ＮＡＮＤ回路を含み、ＡＴＸ電源のＰＳ－ＯＮ入力端子に接続された出力端子を有する請求項２に記載のコンピュータ用電源のセキュリティ制御装置。

2

【請求項６】　前記ンピュータ・システムがパワーオフになると、前記コンピュータ用電源のセキュリティ制御装置および前記キーボードを除く全ての回路系サブシステムは、パワーオフになる請求項２に記載のコンピュータ用電源のセキュリティ制御装置。

【請求項７】　前記コンピュータ・システムがパワーオフになると、前記コンピュータ用電源のセキュリティ制御装置および前記キーボードを除く全ての回路系サブシステムは、パワーオフになり、

前記コンピュータ用電源のセキュリティ制御装置および前記キーボードは、ＡＴＸ電源の５ＶＳＢ待機電源から電力を供給される請求項５に記載のコンピュータ用電源のセキュリティ制御装置。

【請求項８】　前記パスワード・メモリは、不揮発性ランダム・アクセス・メモリ装置からなる請求項２に記載のコンピュータ用電源のセキュリティ制御装置。

【請求項９】　前記パスワード・メモリは、前記コンピュータ・システムのＣＭＯＳ構成メモリ中の指定メモリ・スペースからなる請求項２に記載のコンピュータ用電源のセキュリティ制御装置。

【請求項１０】　前記パスワード・メモリは、前記コンピュータ・システムがオフであるときには、バックアップ・バッテリによってサポートされる静的ランダム・アクセス・メモリからなる請求項２に記載のコンピュータ用電源のセキュリティ制御装置。

【請求項１１】　メインボード回路系、電源、およびキーボードを有するコンピュータ・システム用のパワーアップ・セキュリティ制御を行うコンピュータ用電源のセキュリティ制御装置であって、

前記コンピュータ・システムがオフである時に、前記メインボード回路系のキーボード制御装置インタフェースと前記キーボードとの間で通信するキーボード信号を代行受信するキーボード代行受信ユニットと、

前記キーボード代行受信ユニットが代行受信したキーボード信号を、受信してデコードするキーボード入力データ・デコーダと、

前記キーボード入力データ・デコーダの出力側に供給されたキーボード信号のデコード済みデータを、所定フォーマットで記憶する先入れ先出しバッファと、前記コンピュータ・システムのパワーアップ許可を指定するようにプリセットされたパスワードを記憶するパスワード・メモリと、

前記先入れ先出しバッファおよび前記パスワード・メモリのそれぞれの出力端子に接続された２つの入力端子を有し、前記キーボード信号および前記プリセット・パス

ワードの突合せを比較し、前記比較の突合せ条件を示す信号を生成する比較ユニットと、

論理回路系を含み、前記比較ユニットが生成した突合せ条件を受信して、前記突合せ条件と前記コンピュータ・システムの主電源スイッチ状態との両方に基づき前記論理回路系が実行した論理演算の結果に基づいて制御信号を生成し、前記突合せ条件の結果が正であれば前記コンピュータ・システムの電源をパワーアップするように制御する電源制御ユニットと備えたコンピュータ用電源のセキュリティ制御装置。

【請求項１２】　前記電源は、ＡＴＸ標準に従うものであり、

電源制御ユニットは、前記突合せ条件および前記コンピュータ・システムの主スイッチの論理状態に基づいてＮＡＮＤ演算を実行する論理ＮＡＮＤ回路を含み、ＡＴＸ電源のＰＳ－ＯＮ入力端子に接続された出力端子を有する請求項１１に記載のコンピュータ用電源のセキュリティ制御装置。

【請求項１３】　前記パスワード・メモリは、不揮発性ランダム・アクセス・メモリ装置からなる請求項１１に記載のコンピュータ用電源のセキュリティ制御装置。

【請求項１４】　前記パスワード・メモリは、前記コンピュータ・システムのＣＭＯＳ構成メモリ中の指定メモリ・スペースからなる請求項１１に記載のコンピュータ用電源のセキュリティ制御装置。

【請求項１５】　前記パスワード・メモリは、前記コンピュータ・システムがオフであるときには、バックアップ・バッテリによってサポートされる静的ランダム・アクセス・メモリからなる請求項１１に記載のコンピュータ用電源のセキュリティ制御装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は一般にコンピュータ・システム用の電源制御、とりわけコンピュータ・システムへの電力供給のセキュリティ制御に関する。さらに詳細には、本発明は、システムへの無許可アクセスを制限し、試行アクセスを繰り返すことでシステムが損傷する可能性をシステムをパワーアップすることによって回避する、コンピュータ・システムへの電力供給の効果的なセキュリティ制御に関する。

【０００２】

【従来の技術】通常のマイクロプロセッサ・ベースのパーソナル・コンピュータまたはワークステーション・システムでは、単純な機械オン／オフ接触スイッチを使用して、初期設計のこうしたコンピュータ・システムの電源ユニットへの電力の供給または遮断を実施していた。コンピュータ・システムの電源ユニット中に設置された機械接触スイッチがオフになると、開放回路状態のこのスイッチは電源回路系（circuitry）への電力供給を打ち切り、コンピュータ・システム全体がオフになる。他

方、この主スイッチがオンになると、閉回路状態のスイッチは、家庭用の交流１１０Ｖなどの電力を電源回路系に供給し、ここで交流電力はコンピュータ中の全てのサブシステムへの供給に適した直流電力（正負の直流５および１２ボルトなど）に変換される。必要な全ての直流電力が安定して供給されれば、コンピュータ・システムはそのスタートアップ・シーケンスを開始することができ、その後で起動する。

【０００３】こうした初期コンピュータ・システムで使用される機械接触スイッチは、コンピュータ・システムをオンまたはオフにするために人間の手動操作に依拠する。人間のオペレータが間に入らなければコンピュータはそれ自体をパワーオンまたはオフにすることができない。一方、主電源スイッチが切り替わり、オン状態で維持されると、システムはオペレーションの開始シーケンスを開始および実行することになる。システム・ファームウェア（すなわちｘ８６ベースのＩＢＭ互換コンピュータの場合には基本入出力システム（ＢＩＯＳ））またはオペレーティング・システム・レベルに有効なパスワード制御体系が組み込まれない場合には、パワーアップされた後で、システム全体およびその全てのデータが、このシステムへのアクセス権を有する者に露出される。

【０００４】米国カリフォルニア州Ｃｕｐｅｒｔｉｎｏ のＡｐｐｌｅ　ＣｏｍｐｕｔｅｒＩｎｃ．製のＭａｃｉｎｔｏｓｈシリーズ・モデルのパーソナル・コンピュータでは、キーボード上の指定キーを利用してパワーアップおよびパワーダウンを制御する。ただしこれらは便利ではあるが、初期のＩＢＭ互換機と同様に有効なセキュリティが欠如している。システムの電源コードがユーティリティ・ソケットに接続されると、コンピュータにアクセスすることができる者なら誰でも、キーボード上のパワーアップ・キーを押して簡単にシステムを立ち上げることができる。こうした「ソフト・パワー制御」はシステムのキーボードに触れることができる者なら誰に対しても開かれている。ｘ８６について上述したものと類似したファームウェアおよび／またはオペレーティング・システム・レベルのプログラム・ルーチンを使用して、こうしたコンピュータ・システムに対するアクセス制限を実現しなければならないことになる。

【０００５】他方、米国カリフォルニア州Ｓａｎｔａ ＣｌａｒａのＩｎｔｅｌ　Ｃｏｒｐｏｒａｔｉｏｎは、コンピュータ・システムの直接パワーアップ／ダウン制御のために単純な機械接触スイッチに依拠しない電源サブシステムを有する、ＡＴＸ標準と呼ばれるコンピュータ・マザーボード仕様を提案した。その代わりに、ＡＴＸは、コンピュータ・システム自体に統合された回路系の監視下でのソフト・パワー制御の形態をとる。主電源スイッチ上での単純かつ手動のスイッチオン／オフを超える機能性が、ＡＴＸ標準のマザーボードに提供され、コンピュータ・システムにわたる制御をさらに融通がき

くようにすることができる。

【０００６】例えば、ＡＴＸ仕様バージョン２．０１の場合には、待機電力５ＶＳＢは、最大で０．７アンペアの電流を送る５ボルト直流電源である。これは、主電源が遮断されているときにコンピュータ・システム中のこうした基本電力管理回路系に電力を供給する。これらの電力管理回路系は、コンピュータ・システムの様々な便利な機能を実施するようにプログラムすることができる。例えば、このシステムは、真夜中にオペレータのいない状態でそれ自体を自動的に開始し、その地域の電話会社の割引料金時間中に国際ファクシミリ伝送を送信するようにプログラムすることができる。または、このコンピュータ・システムは、遠隔モデム接続の着信要求によって夕方に覚醒させ、ファイル伝送を受信するようにすることもできる。

【０００７】しかし、ＡＴＸなどのこれらの最近の標準によって実施されるこのようなソフト電力管理の概念では、上述の従来技術のコンピュータ・システムと同様に、適当なセキュリティ措置による決定的なデータ保護の備えが依然として欠如している。ＡＴＸ標準を採用するコンピュータ・システムをユーザ（許可されているか否かに関わらず）が主電源スイッチをオンにして開始すると、電源がオンになり、システムはオペレーションのスタートアップ・シーケンスの実行を開始する。この時点で、システム・ファームウェアまたはオペレーション・システムがどちらもパスワード検査などの適当なセキュリティプログラムを備えていなければ、システムに直接アクセスできる者なら誰でもコンピュータに入っているデータにアクセスすることができる。このようなシステムは、機械主電源スイッチを有する以前の世代のコンピュータと同様に無防備である。

【０００８】ファームウェアまたはオペレーティング・システム・レベルのセキュリティ・システムを備えたこのような従来のコンピュータ・システムが無許可アクセスを受けるときには、システムへの侵入を試みるものは誰でも正しいパスワードを入力しなければならない。しかし、ほとんどの従来のコンピュータ・システムでは簡単なパスワード入力規則を利用している、つまり、ユーザは限られた回数だけパスワードの入力を試みることができる。指定回数だけ試みた後で、無許可ユーザが依然として正しいパスワードを入力することができない場合には、システムは単純にロックすることになる。コンピュータ・システムのキーボードは新しい入力があってもそれ以上応答しなくなる。この場合には、無許可ユーザはコンピュータ・システムへの電力をオフにし、次いで再度これをオンにしなければならない。これは無許可ユーザが新しいパスワード入力ポイントに再度到達することを許す。無許可ユーザがシステムへの侵入を試み続けることを望む場合には、正しいパスワードを入力するまで、このパワーオン／オフのプロセスを繰り返し実行し

なければならない。主電源のスイッチオン／オフを繰り返すこのプロセスの間に、コンピュータ・システムは早く故障する可能性が高くなる。これは、通常のコンピュータ・システムが、このように動作するように設計されていないためである。

【０００９】当業者には周知の通り、マイクロプロセッサ・ベースのコンピュータ・システムは、短い時間周期の間のスイッチオン／オフの繰返しを見込まない、または少なくとも推奨しない電源サブシステム上で動作する。短い時間周期内の連続的なパワーオン／オフ動作は異常動作と考えられるが、これは良好に設計された電源ユニットでは基本的に許容される。こうした電源は、オフになっていた後で、例えば数秒の指定時間周期内にそれ自体がパワーオンすることを防止する保護回路系を備える。コンピュータ・システム中の回路基板は、無許可ユーザがシステムへの侵入を試みた時の連続的なパワーオン／オフ・セッションで起こりうる損傷からこのようにして保護することができるが、ディスク・ドライブなどのその他の構成部品は同様には保護されない。これは、現在のハードディスク・ドライブ用のスピンドル・モータが、このような動作方式用に設計されていないためである。これらは、オンになり、長い時間周期の間パワーオン状態で維持されるようになっている。

【００１０】

【発明が解決しようとする課題】したがって、本発明の目的は、パスワード入力の妥当性に基づいてコンピュータ・システムへの主電力供給を開始するか否かを決定する、コンピュータの電源サブシステム用のセキュリティ制御を行うコンピュータ用電源のセキュリティ制御装置を提供することである。

【００１１】本発明の別の目的は、システムを立ち上げようとする無許可試行によって引き起こされるコンピュータ・システム中の構成部品への潜在的な物理的損傷を防止する、コンピュータの電源サブシステム用のセキュリティ制御を行うコンピュータ用電源のセキュリティ制御装置を提供することである。

【００１２】

【課題を解決するための手段】上記目的を達成するために、本発明は、コンピュータ・システムがオフである時にメインボード回路系のキーボード制御装置インタフェースとキーボードとの間で通信するキーボード信号を代行受信するキーボード代行受信ユニットを含む、コンピュータの電源サブシステム用のセキュリティ制御を行うコンピュータ用電源のセキュリティ制御装置を提供する。キーボード入力データ・デコーダは、キーボード代行受信ユニットが代行受信したキーボード信号を受信し、デコードする。キーボード入力データ・デコーダの出力端子に接続された先入れ先出しバッファは、キーボード信号のデコード済みデータを所定フォーマットで記憶する。パスワード・メモリを使用して、コンピュータ

・システムの許可されたパワーアップを指定するようにプリセットされたパスワードを記憶する。比較ユニットは、それぞれ先入れ先出しバッファおよびパスワード・メモリのそれぞれの出力側に供給された２つの入力を有し、キーボード信号およびプリセット・パスワードの突合せを比較し、この比較の突合せ条件を示す信号を生成する。電源制御ユニットは、比較ユニットが生成した突合せ条件を受信し、突合せ条件の論理状態に基づいて制御信号を生成し、突合せ条件の結果が正であればコンピュータ・システムの電源を制御し、パワーアップする。

【００１３】本発明のその他の目的、特徴、および利点は、下記の好ましいが制限的でない実施形態のさらに詳細な説明によって明らかになるであろう。この説明は、添付の図面に関連して行う。

【００１４】

【発明の実施の形態】図１に示すように、この回路構成は、ｘ８６ベースのＩＢＭ互換パーソナル・コンピュータなどの典型的な従来のコンピュータ・システムのキーボード・インタフェース・セクションが、コンピュータ・システムのコア論理とその外部キーボード・ユニット（ＫＢ）２０との間のインタフェースをとるキーボード制御装置インタフェース（ＫＢＣＩ）１２であることを示す。これは、現在のコンピュータ・システム・ユニットのメインボードまたはマザーボード（ＭＢ）１０が、それから物理的に分離されたキーボード・ユニット２０とインタフェースをとるのに適した設計である。キーボード・ユニット２０は、その内部に設置されたマイクロ制御装置（この図には図示せず）を有する。通常のキーボード・ユニットは人間のタイピングによる入力を処理することしか必要とされないので、したがって、キーボード・ユニット内に設置されたマイクロ制御装置の処理電力を過大にする必要はない。

【００１５】通常は、直列連絡を使用してシステム・ユニットのメインボード１０とコンピュータ・システム中のキーボード・ユニット２０との間の接続を確立する。例えば、図１の例に示す従来技術の回路系の場合には、１対の信号ＫＢＤＡＴＡおよびＫＢＣＬＫを使用して、キーボード・ユニット２０とシステム・ユニット中のマザーボード１０のキーボード制御装置１２との間の接続を確立する。このような直列連絡は、人間のタイピングによる入力を処理する必要を十分に満たす。低電力マイクロ制御装置および直列連絡チャネルを使用することは、コンピュータ・システム全体のコスト削減に有益である。

【００１６】図１に示した従来のコンピュータ・システムには、ＫＢＤＡＴＡおよびＫＢＣＬＫ信号に加えて電力ＶＤＤ経路および接地ＧＮＤ経路も備えられる。無線周波数の干渉を回避するために、この電力供給の対は、通常は適当な分離を介してキーボード２０に供給される。図１の回路系の場合には、キーボード制御装置１２はこの電力を外部キーボード・ユニット２０に供給する。

【００１７】従来のコンピュータ・システムのシステム論理回路系と比較すると、コンピュータの電源サブシステム用の本発明のセキュリティ制御装置は、図１の典型的なコンピュータ・システムに追加することができる独立回路系にすることができる。本発明の好ましい実施形態では、このセキュリティ制御装置は、外部キーボード・ユニット２０とマザーボード１０のキーボード制御装置１２との間に、この２つを接続する信号経路を分岐させて挿入することができる。このような実施態様の実施形態を示すブロック図を図２に見ることができる。図示のように、本発明の実施形態に基づいて構築されたセキュリティ制御装置４０は、コンピュータ・システムの論理回路系中に組み込むことができ、マザーボード１０のキーボード制御装置１２、外部キーボード・ユニット２０、および電源ユニット（ＰＳＵ）３０と対話する。図２は、このような実施態様の構成を示す図である。

【００１８】図面に示すように、本発明を具体化するセキュリティ制御装置４０は、それ自体を、外部キーボード・ユニット２０とコンピュータのマザーボード１０のキーボード制御装置１２との間で通信するキーボード信号ＫＢＤＡＴＡおよびＫＢＣＬＫを代行受信するために使用することができる、独立した回路にすることができる。このセキュリティ制御装置４０は、２つの機能ブロック間で実施される信号通信を監視して、許可されているか否かに関わらず任意のユーザが、有効なパスワードに適合するキーストロークの文字列でキーボード２０を押したかどうかを調べることができる。

【００１９】本発明の好ましい一実施形態では、コンピュータがオフになったときに、セキュリティ制御装置４０は電源ユニット３０によって依然としてパワーオン状態のまま維持され、その設計セキュリティ機能を実施するために必要な電源を有する。ＡＴＸマザーボードの場合には、本発明のセキュリティ制御装置４０は、システムがパワーダウン状態にあるときに５ＶＳＢ電源から電力を供給されることができる。ＡＴＸの５ＶＳＢ電源は、システムがパワーダウン状態にあるときに装置４０が動作してキーボード２０でのキーストロークを監視するのに十分な電流を供給することができる。一方、電源ユニット３０もまた、キーストローク走査回路系がキーボード・マイクロ制御装置の制御下で動作するのに十分な電力を外部キーボード・ユニット２０に供給する必要がある。

【００２０】正当な権利を有する、またはコンピュータ・システムへの侵入を試みるユーザが外部キーボード２０を介してキーストロークを押し、プリセット・パスワードに適合する文字列をコンピュータ・システムに入力しようとする際に、セキュリティ制御装置４０は押されたキーストロークを監視し、それらと事前に記憶したパ

スワードとを比較することができる。記憶したパスワードと入力されたキーストロークの比較の結果が正であれば、セキュリティ制御装置４０はイネーブル信号を生成し、電源ユニット３０をオンにすることができ、次いでこれがコンピュータ・システム全体を開始し、立ち上げる。

【００２１】電源ユニット３０がオンになった後で、コンピュータ・システムは通常のブートアップ・シーケンスを続行することができ、コンピュータは通常通り機能することができる。例えば、ＡＴＸの仕様の下では、セキュリティ制御装置４０が入力されたキーストローク文字列が有効なパスワードであると決定したときに、装置４０が生成したイネーブル信号をＡＴＸ電源ユニット３０中のＰＳ－ＯＮ入力端子に結合することができる。ＡＴＸ電源３０のＰＳ－ＯＮ入力端子に送信される論理的に正すなわち論理的に低レベルの信号は、電源ユニットをオンにし、次いでこれがコンピュータ・システムをパワーアップすることに、当業者なら気づくであろう。

【００２２】他方、セキュリティ制御装置４０が、押されたパスワードのキーストロークが有効でないと決定した場合には、ＡＴＸ電源３０へのＰＳ－ＯＮ入力は論理的に負の状態で維持される。論理的に高レベルの信号はＡＴＸ電源ユニット３０をパワーオフ状態で維持する。この場合には、外部キーボード・ユニット２０およびセキュリティ制御装置４０を除けば、ＣＰＵ、ディスク・サブシステム、およびマザーボード１０中のキーボード制御装置１２も含めたコンピュータ・システム全体が全てオフに維持される。換言すれば、侵入者がコンピュータ・システムの外部キーボード・ユニット２０上で何を何回試みるかに関わらず、正しいパスワードが与えられない限り電源ユニット３０はパワーダウン状態に保たれる。電源ユニット３０がオフに維持されるので、コンピュータ・システムの重要な構成部品、とりわけ精密で比較的脆弱なディスク・サブシステムが、パスワード推測セッションを繰り返すプロセス中に、急速にパワーアップおよびパワーダウンを繰り返されることはなくなる。急速なパワーオン／オフ・サイクルの結果としてコンピュータ構成部品に損傷が与えられる可能性は、このようにしてほぼ回避することができる。

【００２３】好ましい実施形態では、本発明のセキュリティ制御装置４０は、マザーボード１０のキーボード制御装置１２に中継することができる別の制御信号ＳＷの生成をさらに含むことができる。コンピュータ・システムがパワーダウン状態にあるときには、この信号により、セキュリティ制御装置４０はキーボード信号ＫＢＤＡＴＡおよびＫＢＣＬＫを代行受信し続け、キーボード２０上で押された場合にパスワード入力の妥当性を監視することができる。他方、コンピュータ・システムがうまく（すなわち、有効なパスワードの正しい入力によって）パワーオンになったときに、制御信号ＳＷを使用して、キーボード信号ＫＢＤＡＴＡおよびＫＢＣＬＫの通常の流れを、従来のコンピュータ・システムでは通常である、キーボード制御装置１２および外部キーボード・ユニット２０に復帰させることができる。

【００２４】しかし、コンピュータ・システムがオフである間に、セキュリティ制御装置４０がキーが押される状態を外部キーボード・ユニット２０にわたって絶えず監視する際には、図２の場合と同様に、キーボード・ユニット２０への電力供給ＶＫＢはＡＴＸ電源ユニット３０の待機電力５ＶＳＢから供給される。これは、マスタ・オフ状態中にＡＴＸの主５ボルト供給ＶＤＤが遮断されるので必要である。しかし、待機５ボルト電力５ＶＳＢは、マスタ・オフ状態中に活動状態を維持し、指定された駆動能力を提供することができる。コンピュータ・システムが通常通りパワーオンになった後で、外部キーボード・ユニットへの電力は待機電力５ＶＳＢからマスタ電力ＶＤＤに切り替わることができる。ただし、コンピュータ・システムが通常通りブートアップした後で、外部キーボード・ユニットが待機電力から電力を供給されたままにすることも同様に可能である。

【００２５】本発明のセキュリティ制御装置用の回路系の好ましい実施形態について以下で考察する。図３は、本発明の好ましい実施形態によるセキュリティ制御装置の回路系構成を示すブロック図である。この図に示すように、この装置は一般に、キーボード入力データ・デコーダ（ＫＢＤＥＣ）４１、先入れ先出し（ＦＩＦＯ）バッファ４２、パスワード・メモリ（PWM）４３、比較ユニット（ＣＬ）４４、キーボード代行受信ユニット（ＫＢＩＬ）４５、および電源制御ユニット（ＰＳＣＬ）４６を含む。

【００２６】最初に、キーボード代行受信ユニット４５が、コンピュータ・システムのパワーアップ／ダウン状態に基づいてキーボード信号代行受信制御信号ＳＷを生成する。好ましい実施形態では、キーボード代行受信ユニット４５は、コンピュータ・システムのパワーオン／オフ状態のそれぞれを表す逆の論理状態を有する論理信号ＳＷを単純に生成する論理回路にすることができる。コンピュータ・システムがパワーオフ状態にあるときには、１つの論理状態を有するＳＷ信号を使用して、キーボード信号ＫＢＤＡＴＡおよびＫＢＣＬＫの代行受信を制御して監視することができる。他方、コンピュータ・システムがパワーオン状態にあるときには、逆の論理状態を有するＳＷ信号を使用して、図２のブロック図に示す、外部キーボード・ユニット２０とマザーボード１０のキーボード制御装置１２との間の通常のキーボード信号通信に復帰させることができる。

【００２７】例えば、好ましい実施形態では、各キーボード信号ＫＢＤＡＴＡおよびＫＢＣＬＫごとに１つの３状態バッファを使用して、外部キーボード・ユニット２０とコンピュータ・システムのマザーボード１０のキー

ボード制御装置１２との間でこの対の信号制御を代行受信するか否かの制御を容易にすることができる。図４は、本発明の好ましい実施形態によるセキュリティ制御装置の回路系構成の概略図である。本発明の装置はキーボード信号ＫＢＤＡＴＡおよびＫＢＣＬＫを代行受信して、コンピュータ・システムを立ち上げるのに有効なパスワードをシステムが受信したか否かを決定する。図示のように、キーボード制御装置インタフェース１２は、通常のＩＢＭ互換コンピュータではＩｎｔｅｌ　８０４２／８０４８　８ビット・マイクロ制御装置またはその同等物となる典型的なマイクロ制御装置１２０を含む。ＩＢＭ互換システムのキーボード制御装置インタフェース１２では、このインタフェースを制御するマイクロ制御装置１２０は、オープン・コレクタ・バッファを介してキーボード信号ＫＢＤＡＴＡおよびＫＢＣＬＫをそれぞれ出力するＰ２７およびＰ２６ポートのそれぞれを有する。本発明のセキュリティ制御装置を利用するコンピュータ・システムでは、これら２つのオープン・コレクタ・バッファを１対の３状態バッファ１２１および１２２とそれぞれ交換することができる。

【００２８】図４に示すように、好ましい実施形態での２つの３状態バッファ１２１および１２２は、外部キーボード・ユニット２０に電力を供給する同一の電源ＶＫＢから電力を供給されることができる。これは、これら２つのバッファが、外部キーボード・ユニット自体とともに活動状態のまま残らなければならないためである。

【００２９】コンピュータ・システムがパワーダウンした時、セキュリティ制御装置４０のキーボード代行受信ユニット４５は、論理的に低レベルの制御信号ＳＷを生成する。図４に示す好ましい実施形態で利用する３状態バッファ１２１および１２２は論理的に正のイネーブル入力制御を有するので、したがって、論理的に低レベルの制御信号ＳＷは両バッファを高インピーダンスのオフ状態にする。このような状況下では、バッファの入力端子の後ろにある回路系は、それぞれのキーボード信号線ＫＢＤＡＴＡおよびＫＢＣＬＫから実質的に遮断されたものと考えることができる。他方、正しいパスワードが入力された結果としてコンピュータ・システムがパワーアップした時には、キーボード代行受信ユニット４５はその論理的高レベル状態で対応する制御信号ＳＷを生成する。このバージョンの制御信号ＳＷは、マイクロ制御装置１２０のＰ２７およびＰ２６ポートを外部キーボード・ユニット２０に効果的に接続する。この接続は、キーボード信号ＫＢＤＡＴＡおよびＫＢＣＬＫでそれぞれ活動化される３状態バッファ１２１および１２２の対を介して行われる。これにより、外部キーボード・ユニット２０とコンピュータ・システムのマザーボード１０との間の通常の電気信号接続が効果的に確立される。

【００３０】このようにして、上記の好ましい実施形態では、キーボード代行受信ユニット４５を、単純に電源

ユニット３０の主５ボルト電源ＶＤＤで交換することができる。換言すれば、キーボード・インタフェース用の２つの３状態バッファ１２１および１２２の出力イネーブル制御入力は、直接、または適当に選択したプルアップ・レジスタを介して、ＶＤＤに結合することができる。

【００３１】次いで再度図３を参照すると、コンピュータ・システムがパワーダウン状態になっているので、キーボード代行受信ユニット４５はキーボード信号ＫＢＤＡＴＡおよびＫＢＣＬＫを代行受信し、セキュリティ制御装置４０中に切り替えることができる。代行受信されたキーボード信号は、このようにしてキーボード入力データ・デコーダ４１に直接送信し、デコードすることができる。次いでデコーダ４１は、キーボード信号として表される受信した英数文字を、コンピュータ・システムで使用される標準コードに順次変換することができる。次いで、入力されたキーストロークを表すこれらの変換されたコードは、先入れ先出しバッファ４２に送られて所定のデータ・ファーマットで記憶され、後続の処理を待機する。

【００３２】他方、適当な動作手続きを予め実行しておくことにより、指定パスワードをパスワード・メモリ４３に記憶することができる。本発明の好ましい実施形態では、このパスワード・メモリ４３は、電力がなくなった後もその記憶情報を永久的に維持することができる不揮発性ランダム・アクセス・メモリ（ＮＶＲＡＭ）装置にすることができる。あるいは、ＩＢＭ互換コンピュータの場合には、パスワード・メモリ４３は、コンピュータ・システムのハードウェア構成を記録する情報を維持するために使用されるＣＭＯＳメモリ中の指定メモリ・スペースにすることもできる。別の実施形態では、パスワード・メモリ４３は、コンピュータ・システムがパワーダウンした後でそのメモリ内容を維持するためにバックアップ・バッテリを有する、単純な静的ランダム・アクセス・メモリ（ＳＲＡＭ）にすることもできる。

【００３３】パスワード入力によってコンピュータ・システムの電源を活動化するプロセスでは、パスワードは、例えばリターンキーを押すことによって確定することができる。換言すれば、パスワードに使用できないキーであるリターンキーを使用して、パスワードの文字列入力の終了を表明することができる。この表明キー信号を受信すると、次いでコンピュータ・システムのファームウェア・ルーチンを開始して、先入れ先出しバッファ４２およびパスワード・メモリ４３のそれぞれから、入力されたパスワード入力を比較ユニット４４にロードし、これを事前に記憶した有効パスワードと比較することができる。この比較の結果、比較ユニット４４はパスワード突合せ信号ＰＭを生成し、次いでこれが電源制御ユニット４６に中継される。

【００３４】パスワード突合せ信号ＰＭの論理状態に基

づいて、電源制御ユニット４６は、コンピュータ・システムの電源ユニットと直接インタフェースをとり、これを制御するために使用することができる電源制御信号を生成する。例えば、ＡＴＸ電源の場合には、この生成された電源制御信号は、ＡＴＸ電源のＰＳ－ＯＮ入力端子に直接結合することができる、ＡＴＸ仕様に従う論理的に負のＰＳ－ＯＮ信号にすることができる。ＡＴＸ電源の場合には、ＰＳ－ＯＮ入力端子における論理的に高レベルの信号は、電源をオフ状態のまま保つ。他方、ＰＳ－ＯＮ入力での論理的に低い信号は、電源を活動化させ、コンピュータ・システムを無条件で立ち上げる。

【００３５】好ましい実施形態では、コンピュータ・システムのその他の制御論理から得られるさらに別の制御信号を、電源制御ユニット４６に中継することができる。これらの追加制御信号は、電源制御信号、すなわちＡＴＸ電源ユニット３０を制御するために使用される図３の例に示すＰＳ－ＯＮ信号の生成プロセスの寄与要素として使用することができる。例えば、コンピュータ・システムが主電源スイッチを備える場合には、このスイッチの論理的オン／オフ状態を示すために使用する信号ＭＳＷを、この図に示すように電源制御ユニット４６に入力することができる。パスワード突合せＰＭ信号および主スイッチ状態ＭＳＷ信号の両方について論理的に正と取り決めた場合には、電源制御ユニット４６で両信号について論理ＮＡＮＤ演算が実施され、論理的に負のＰＳ－ＯＮ出力が得られる。

【００３６】例示を目的として、好ましい実施形態に関連して本発明について説明したが、本発明は必ずしも開示の実施形態に限定される必要はないことは理解されるであろう。例えば、通常のＩＢＭ互換コンピュータ・システムでは、単純な８ビット・マイクロ制御装置を利用して、システム・マザーボード上のキーボード・インタフェース制御を実施している。したがって、これらのｘ８６ベースのコンピュータで使用される代表的な外部キーボード・ユニットは、対応して互換性のある処理能力を有するマイクロ制御装置を利用して、独立したキーボード・ユニットの制御を実施することができる。キーボード・インタフェースの両端子にあるマイクロ制御装置は、互いに直列接続で通信する。ただし、本発明の実施態様では、その他の形態のこの２つの間の通信も可能である。

【００３７】例えば、キーボード・インタフェース・マイクロ制御装置が常駐するＸＡ／ＸＤ周辺バス上にはその他の周辺機器も存在するので、ＩＢＭ互換コンピュータの場合に使用する従来のＩｎｔｅｌ　８０４２／８０４８デバイスを、さらに高性能のマイクロ制御装置と交換することが必要になることもある。このような状況でも、本発明のセキュリティ制御装置は依然として適用可能である。

【００３８】一方、現在のパーソナル・コンピュータはＡＳＩＣ（アプリケーション特定ＩＣ）デバイスを中心に構築されるので、本発明のセキュリティ制御装置は、こうしたＡＳＩＣ回路系でも実行可能であり、コンピュータ・システムのコア論理チップセット中に含めることができる。したがって、本発明のセキュリティ制御装置の論理回路系はコンピュータのコア論理と比較して比較的単純であるので、本発明の装置をコンピュータのコア論理ＡＳＩＣデバイスに組み込むことで、全体的なゲート・カウントが顕著に追加されることはほとんどない。換言すれば、ＡＳＩＣデバイスに本発明の装置を組み込んでも、半導体製造の総コストはそれほど追加されない。他方、このセキュリティ制御装置は比較的単純な論理回路系を有するので、消費される電力は少量である。換言すれば、本発明のセキュリティ制御装置を組み込むことは、ＡＴＸ仕様などの電源ユニット中の待機電源に非常に適している。

【００３９】さらに、ＡＴＸ仕様の電源ユニットに加えて、ＮＬＸやＰＳ／２など、ソフト電力制御を実施するイネーブル入力を特徴とするその他の標準も、全て同様に適用可能である。

【００４０】したがって、上記の説明部分は、添付の請求の範囲の趣旨および範囲内に含まれる様々な修正形態および類似配列をカバーするものとし、その範囲は最も広範な解釈に一致し、このような修正形態および類似構造を全て包含するものとする。

【図面の簡単な説明】

【図１】　従来のコンピュータ・システム中の対応する外部キーボード・ユニットとのインタフェースをとるキーボード制御装置の回路構成を示す、簡略化したブロック図である。

【図２】　キーボード制御装置がコンピュータ・システム中の対応する外部キーボード・ユニットとのインタフェースをとるための、本発明の好ましい実施形態によるセキュリティ制御装置を利用する回路構成を示すブロック図である。

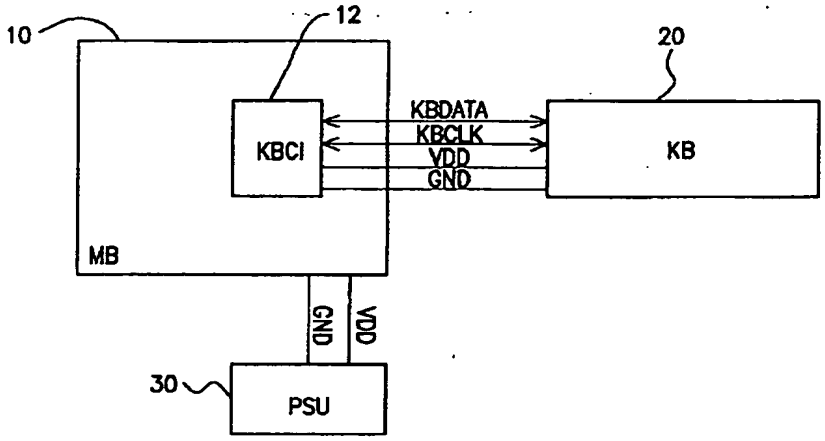
【図３】　本発明の好ましい実施形態によるセキュリティ制御装置の回路構成を示すブロック図である。

【図４】　本発明の好ましい実施形態によるセキュリティ制御装置の回路構成を示す概略図である。

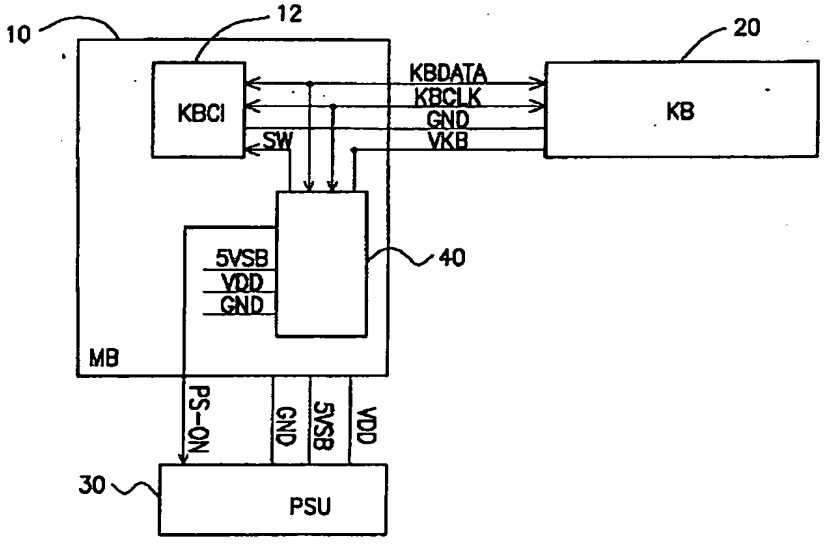
【符号の説明】

４０　セキュリティ制御装置、４１　キーボード入力データ・デコーダ、４２先入れ先出しバッファ、４３　パスワード・メモリ、４４　比較ユニット、４５　キーボード代行受信ユニット、４６　電源制御ユニット。

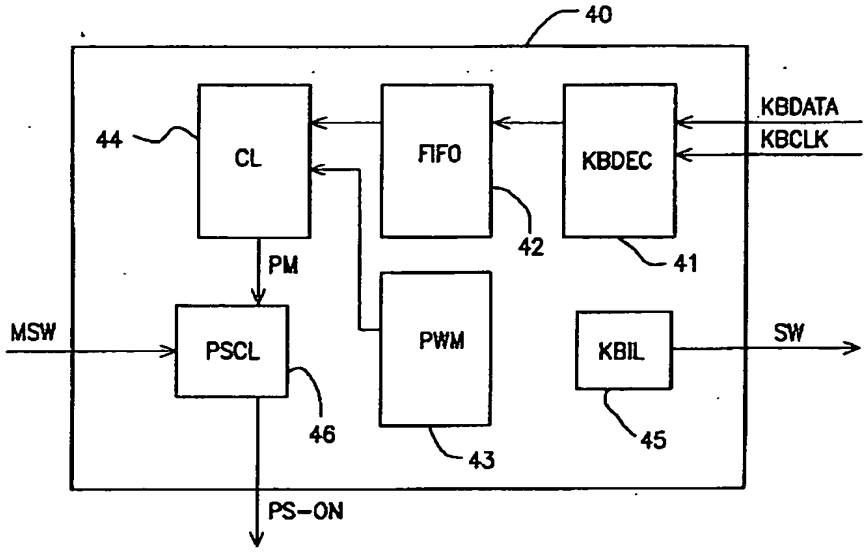
【図１】


10
12
20
KBCI
KBDATA
KBCLK
VDD
GND
KB
MB
GND
VDD
30
PSU

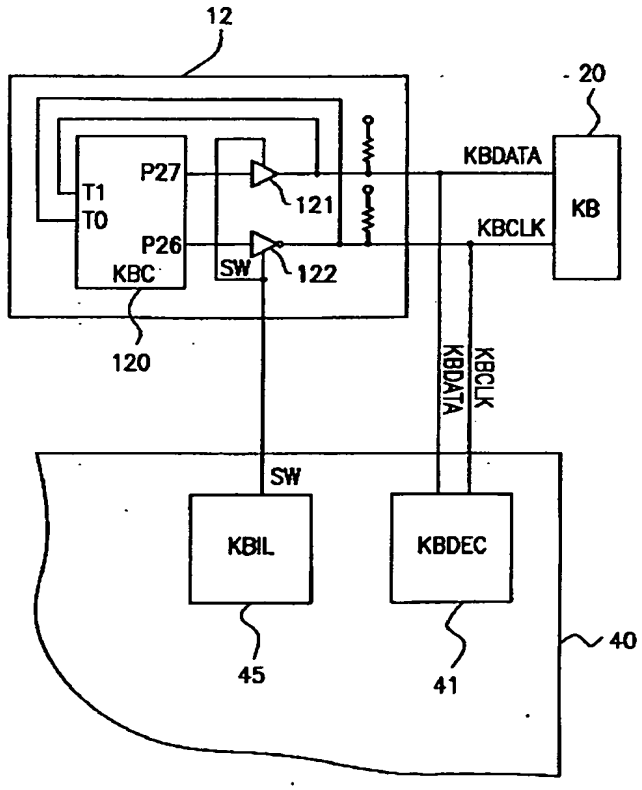
【図２】


10
12
20
KBCI
KBDATA
KBCLK
GND
VKB
KB
SW
5VSB
VDD
GND
40
MB
PS-ON
GND
5VSB
VDD
30
PSU

【図３】


40
44
CL
FIFO
KBDEC
KBDATA
KBCLK
42
41
PM
MSW
PSCL
PWM
KBIL
SW
46
43
45
PS-ON

【図４】


12
20
T1
T0
P27
P26
KBC
SW
121
122
KBDATA
KBCLK
KB
120
KBDATA
KBCLK
SW
KBIL
KBDEC
45
41
40